SNMP/HTTP Access Control User Manual

1. Security Control Configuration 3
1.1. HTTP Security 3
1.1.1. HTTP Security disabled 3
1.1.2. HTTP Security enabled 4
1.1.3. HTTP Security Control 5
1.2. IP Firewall Table 7
1.2.1. NMS IP Address 7
1.2.2. Community 9
1.2.3. Access Type 9
1.3. Reset Access Control Table 11
2. How to filter 12
2.1. Host 12
2.2. Network segment 13
2.3. Allow one IP address to login in segment 14
Appendix A –Behavior flow chart 15
Appendix B – What is IP/CIDR 17

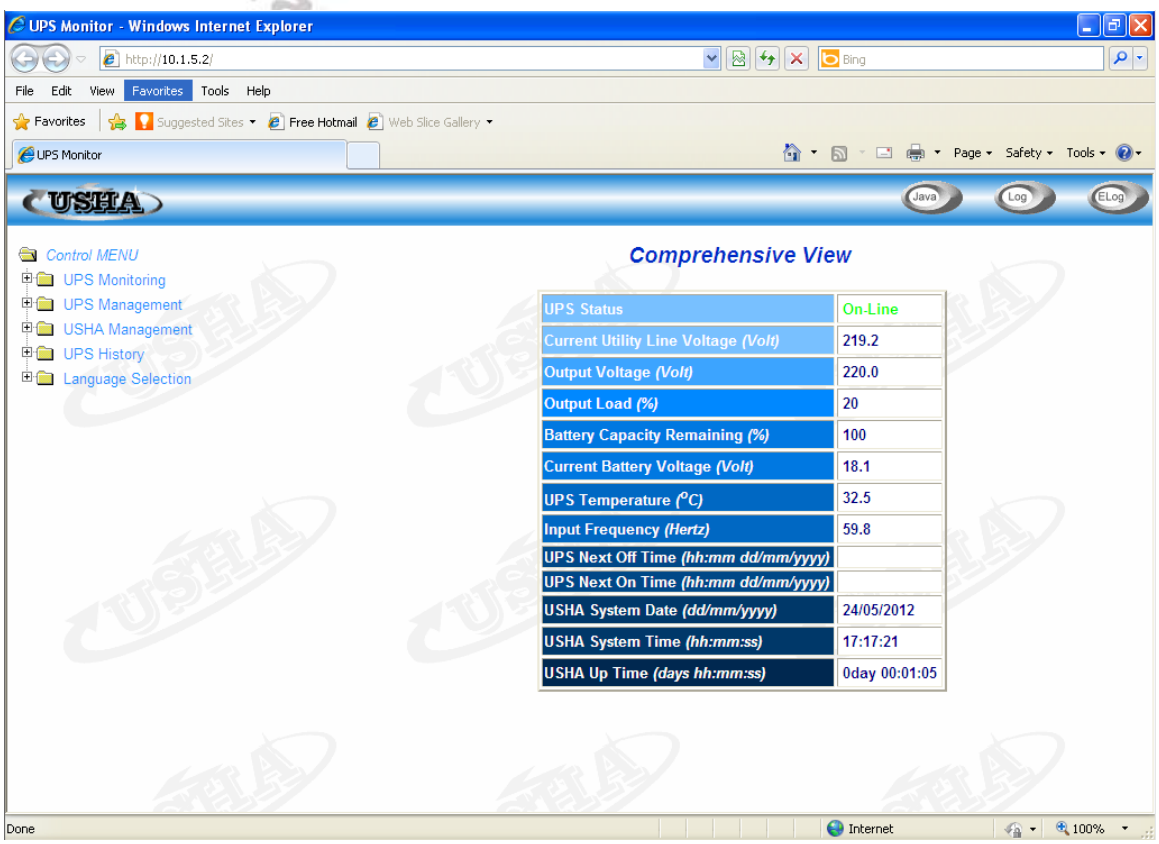
1. Security Control Configuration

1.1. HTTP Security

1.1.1. HTTP Security disabled

```
+=============================================================================+
|                        [ HTTP Configuration Menu ]                          |
+=============================================================================+
   1. HTTP Control            : Enabled
   2. HTTP Port               : 80
   3. HTTP Security Control   : Disabled
   4. UPnP Control            : Disabled
   5. HTTP(s) Authentication  : Local User
   0. Return to previous menu
```

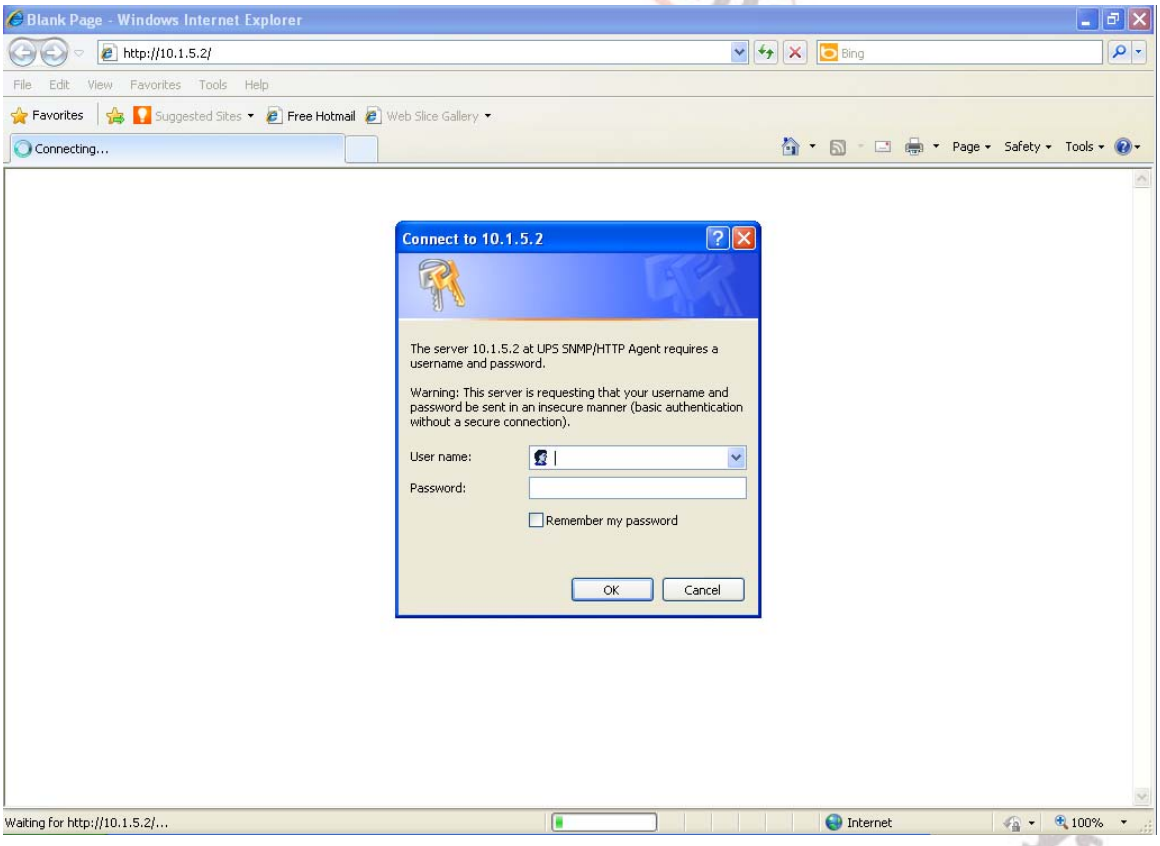
Default is HTTP security disabled. When HTTP security is disabled, the login windows would not popup immediately. Host can connect to USHA directly. If you set access type is “Not Access” and HTTP security is disabled, host still can access to USHA via HTTP.



1.1.2. HTTP Security enabled

```
+=============================================================================+
|                        [ HTTP Configuration Menu ]                          |
+=============================================================================+
   1. HTTP Control            : Enabled
   2. HTTP Port               : 80
   3. HTTP Security Control   : Enabled
   4. UPnP Control            : Disabled
   5. HTTP(s) Authentication  : Local User
   0. Return to previous menu
```

If HTTP security is enabled, will popup login windows immediately when host connect to USHA. We suggest make HTTP security is enabled and configuration access control function, and then you can have higher security.


Blank Page - Windows Internet Explorer
http://10.1.5.2/
Connecting...
Connect to 10.1.5.2
The server 10.1.5.2 at UPS SNMP/HTTP Agent requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
User name:
Password:
Remember my password
OK
Cancel
Waiting for http://10.1.5.2/...
Internet
100%

1.1.3. HTTP Security Control

1. Launch hyper-terminal or telnet connect to USHA, then enter password.
2. Go to “USHA Configuration”.

```
+=============================================================================+
|                 [ USHA Configuration Utility Main menu ]                    |
+=============================================================================+
   1. USHA Configuration
   2. UPS Parameters
   3. Access Control Table
   4. Domain User Table
   5. Trap Receiver Table
   6. SNMPv3 USM Table
   7. Reset Configuration To Default
   8. Restart USHA
   9. UPS Pass-Through
   0. Exit

Please Enter Your Choice => 1


+=============================================================================+
|                       [ USHA Configuration Menu ]                           |
+=============================================================================+
   1. System Group
   2. Control Group
   3. Parameter Group
   4. Email Group
   5. Web Authentication Group
   6. Ping Group
   0. Return to previous menu
```

3. Go to “Control Group”.

```
+=============================================================================+
|                       [ USHA Configuration Menu ]                           |
+=============================================================================+
   1. System Group
   2. Control Group
   3. Parameter Group
   4. Email Group
   5. Web Authentication Group
   6. Ping Group
   0. Return to previous menu

Please Enter Your Choice => 2


+=============================================================================+
|                   [ Control Group Configuration Menu ]                      |
+=============================================================================+
   1. HTTP Login Username       : USHA
   2. Community Read-Only       : public
   3. Community Read/Write      : *
   4. BOOTP/DHCP Control        : Disabled
   5. TFTP/HTTP Upgrade Control : Enabled
   6. PING Echo Control         : Enabled
   7. Telnet Control
   8. HTTP Control
   9. SNMP Control
   A. SMTP Port                 : 25
   B. SSH Control
   0. Return to previous menu
```

4. Go to “HTTP Control”.

```
+=============================================================================+
|                    [ Control Group Configuration Menu ]                     |
+=============================================================================+
   1. HTTP Login Username       : USHA
   2. Community Read-Only       : public
   3. Community Read/Write      : *
   4. BOOTP/DHCP Control        : Disabled
   5. TFTP/HTTP Upgrade Control : Enabled
   6. PING Echo Control         : Enabled
   7. Telnet Control
   8. HTTP Control
   9. SNMP Control
   A. SMTP Port                 : 25
   B. SSH Control
   0. Return to previous menu

Please Enter Your Choice => 8


+=============================================================================+
|                        [ HTTP Configuration Menu ]                          |
+=============================================================================+
   1. HTTP Control           : Enabled
   2. HTTP Port              : 80
   3. HTTP Security Control  : Enabled
   4. UPnP Control           : Disabled
   5. HTTP(s) Authentication : Both
   0. Return to previous menu
```

5. Set “HTTP Security Control” is enabled.

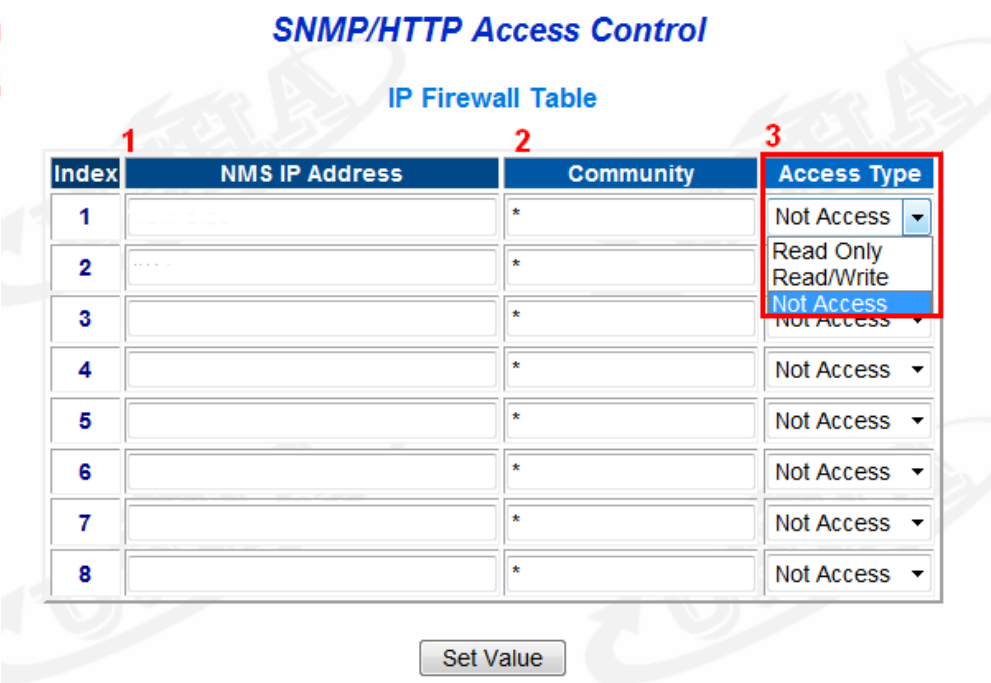
```
+=============================================================================+
|                        [ HTTP Configuration Menu ]                          |
+=============================================================================+
   1. HTTP Control           : Enabled
   2. HTTP Port              : 80
   3. HTTP Security Control  : Disabled
   4. UPnP Control           : Disabled
   5. HTTP(s) Authentication : Both
   0. Return to previous menu

Please Enter Your Choice => 3
Enable/Disable HTTP Security - [Disabled]
   1. Enable
   2. Disable

Please Enter Your Choice => 1


+=============================================================================+
|                        [ HTTP Configuration Menu ]                          |
+=============================================================================+
   1. HTTP Control           : Enabled
   2. HTTP Port              : 80
   3. HTTP Security Control  : Enabled
   4. UPnP Control           : Disabled
   5. HTTP(s) Authentication : Both
   0. Return to previous menu
```

1.2. IP Firewall Table

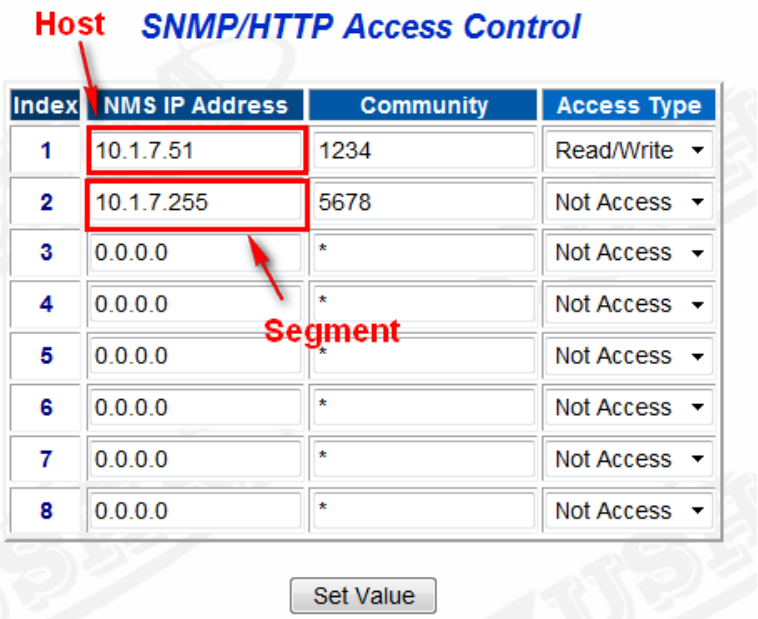


1.2.1. NMS IP Address

This field used to set an IP address or a network segment. You can management this IP or segment according to access type.

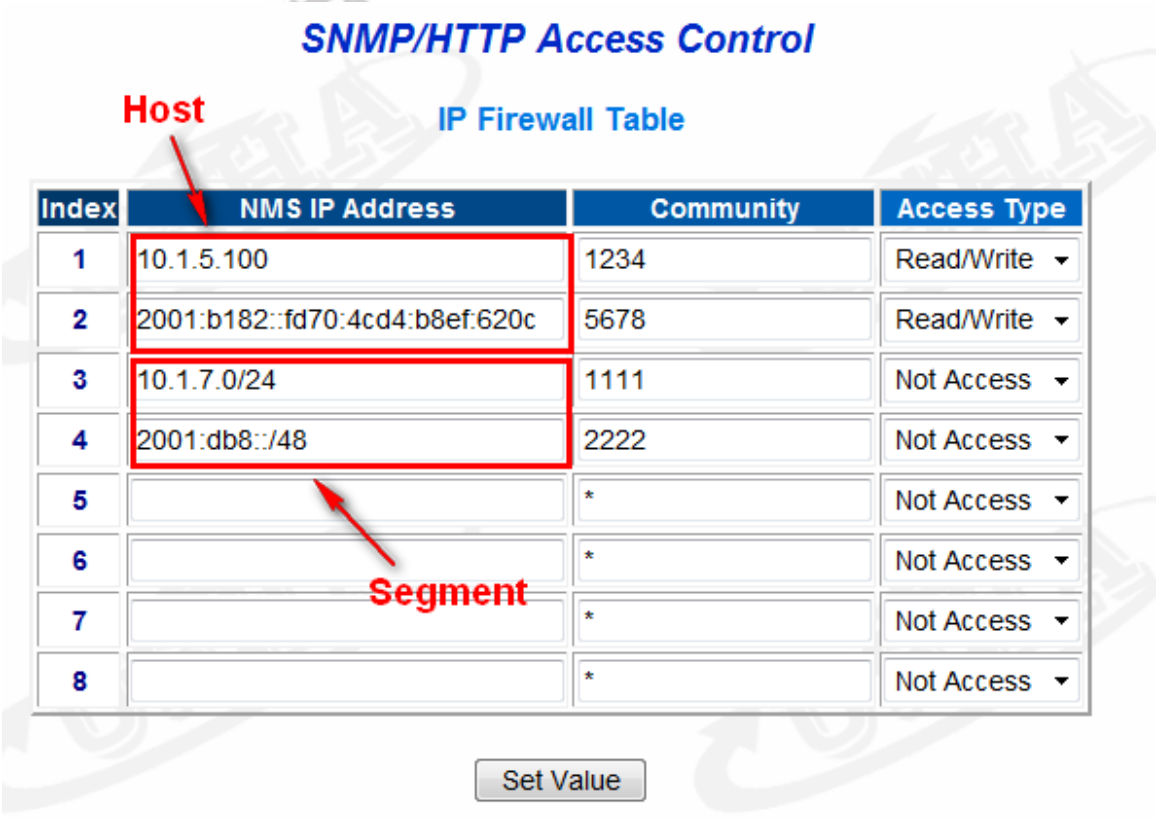
1.2.1.1. USHA 5.x

In USHA 5.x, this field only can set IPv4 address. If you want to set a network segment, you can set **10.1.7.255** that mean the client with the IP address within the range from 10.1.7.0 to 10.1.7.255.



1.2.1.2. USHA 6.x

In USHA 6.x, this field can set IPv4 and IPv6 address. If you want to set a network segment, you can set **10.1.7.0/24** that mean the client with the IP address within the range from 10.1.7.0 to 10.1.7.255. If used IPv6, you can set 2001:db8::/48 that mean the client with the IP address within the range from 2001:db8:0:0:0:0:0:0 to 2001:db8:0:ffff:ffff:ffff:ffff:ffff.



1.2.2. Community

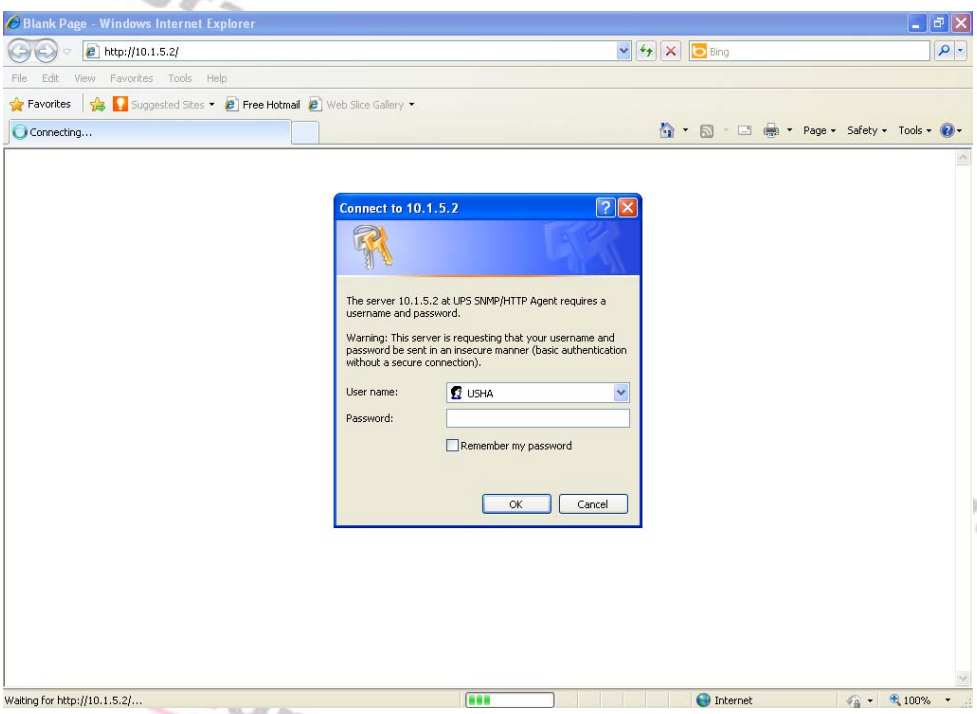
This field used to define a password. When used this password login, host will according access type connect to USHA web page. This field default value is “public”. If you do not set community and access type set “Not Access” or “Read only”, this host will not be able to login. If you can’t login due to this situation, you can use telnet or hyper-terminal to reset this item.

1.2.3. Access Type

This field used to define this IP address access type. There have “**Not Access**”, “**Read Only**” and “**Read/Write**” three types.

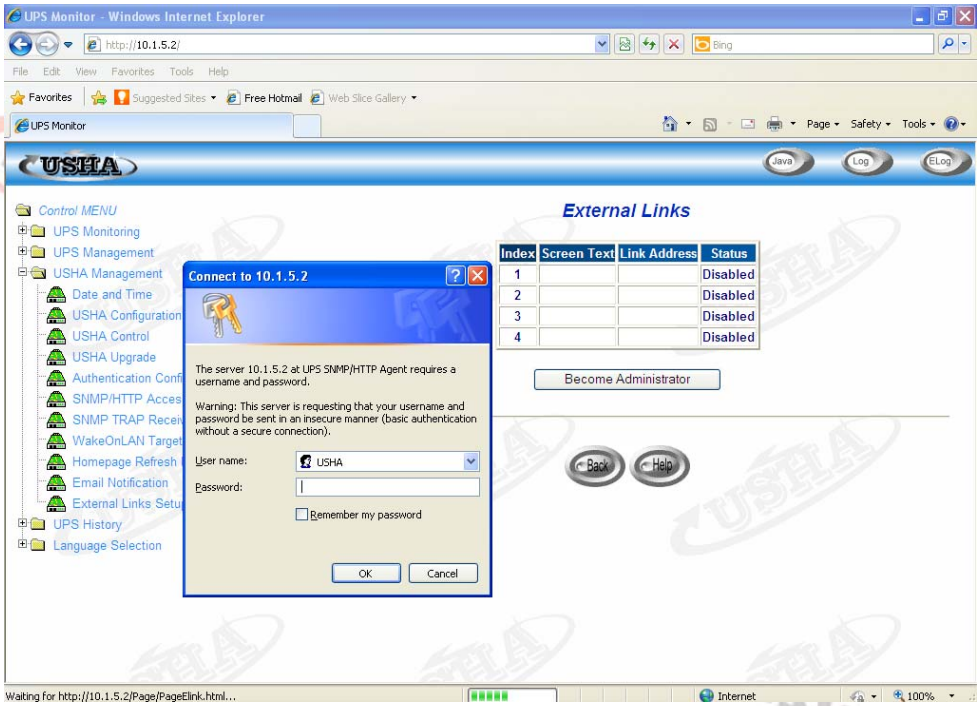
1.2.3.1. Not Access

When access type is “Not Access” and HTTP Security Control is enabled, host would not access web page. When access type is “Not Access” and HTTP Security Control is disabled, host can access web page but read only.



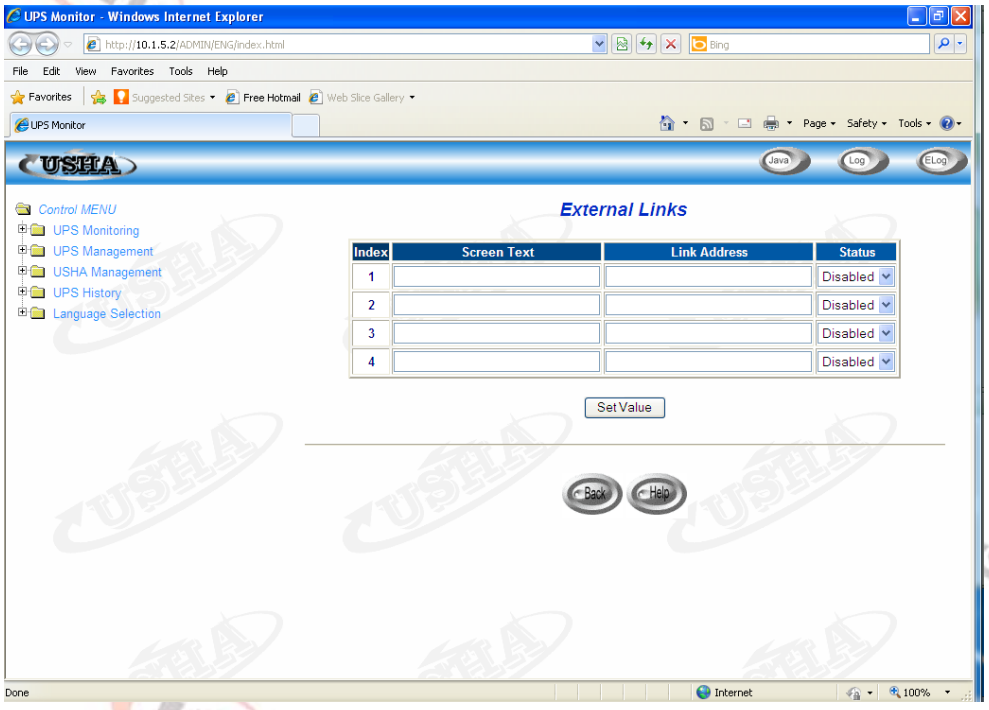
1.2.3.2. Read Only

Host can access web page but read only.



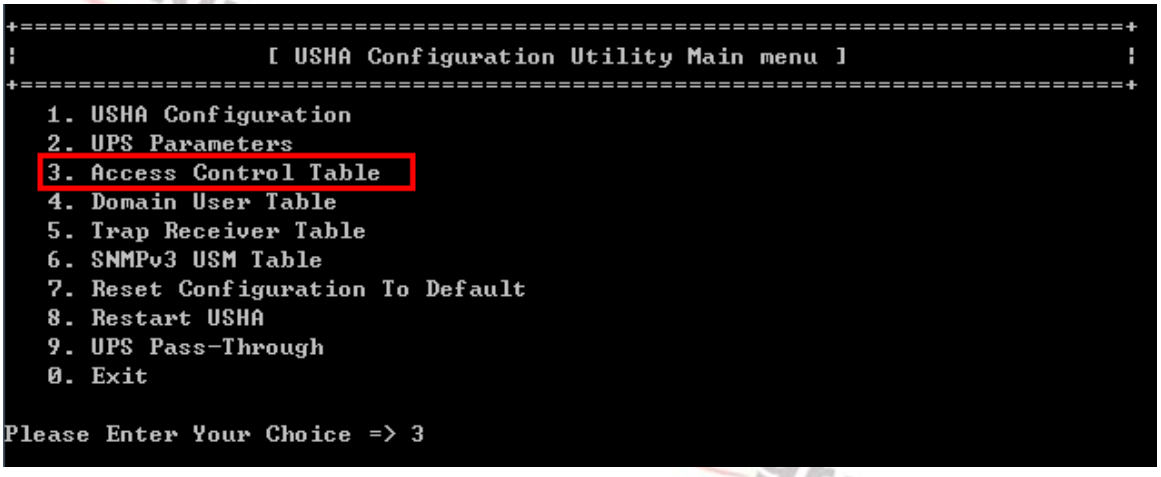
1.2.3.3. Read/Write

Host can access web page and configuration all parameter.

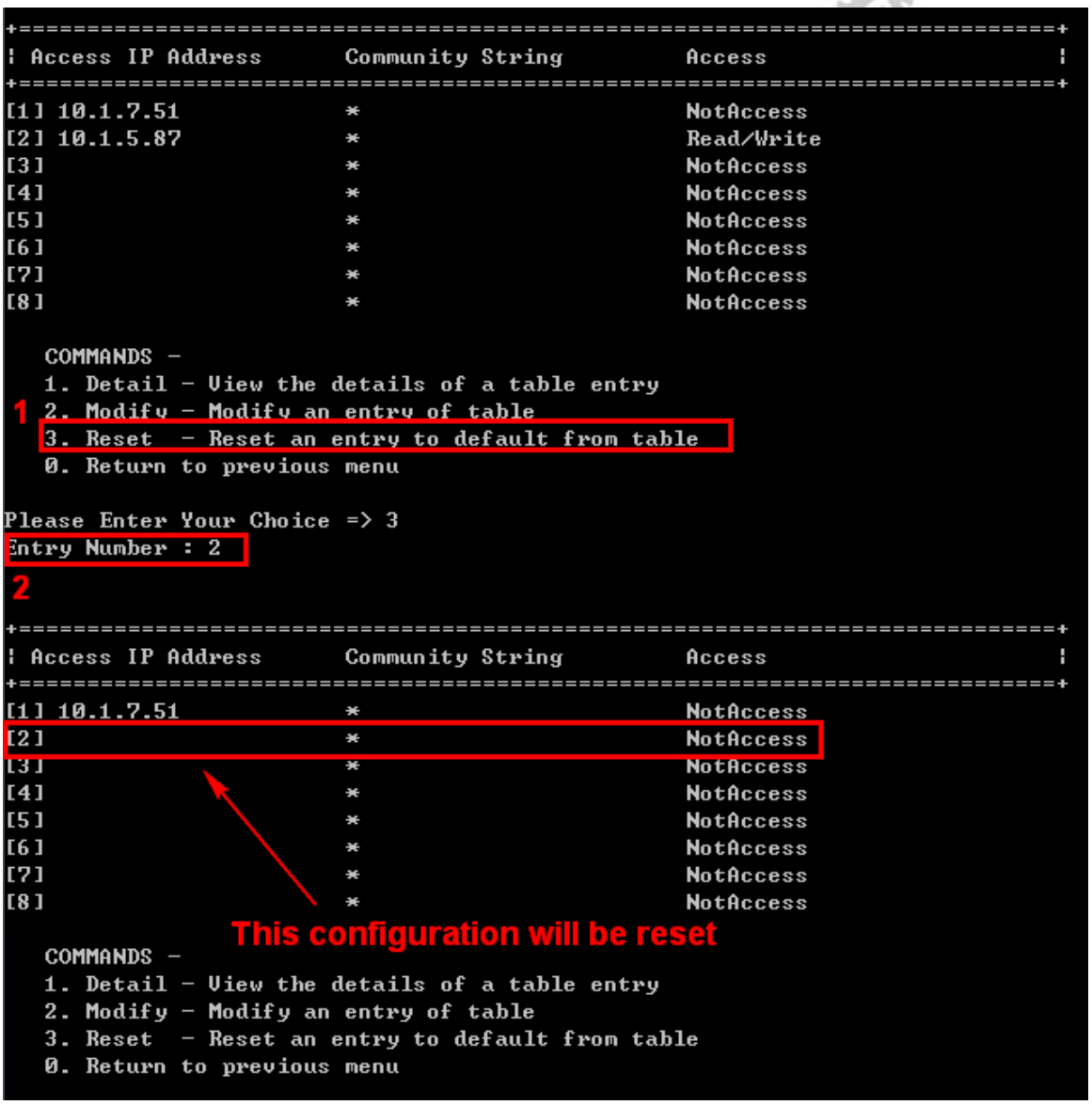


1.3. Reset Access Control Table

1. Launch hyper-terminal or telnet connect to USHA, then enter password.
2. Go to “Access Control Table”.


[USHA Configuration Utility Main menu]
1. USHA Configuration
2. UPS Parameters
3. Access Control Table
4. Domain User Table
5. Trap Receiver Table
6. SNMPv3 USM Table
7. Reset Configuration To Default
8. Restart USHA
9. UPS Pass-Through
0. Exit
Please Enter Your Choice => 3

3. Select “Reset”, and then entry index number that you want to reset.

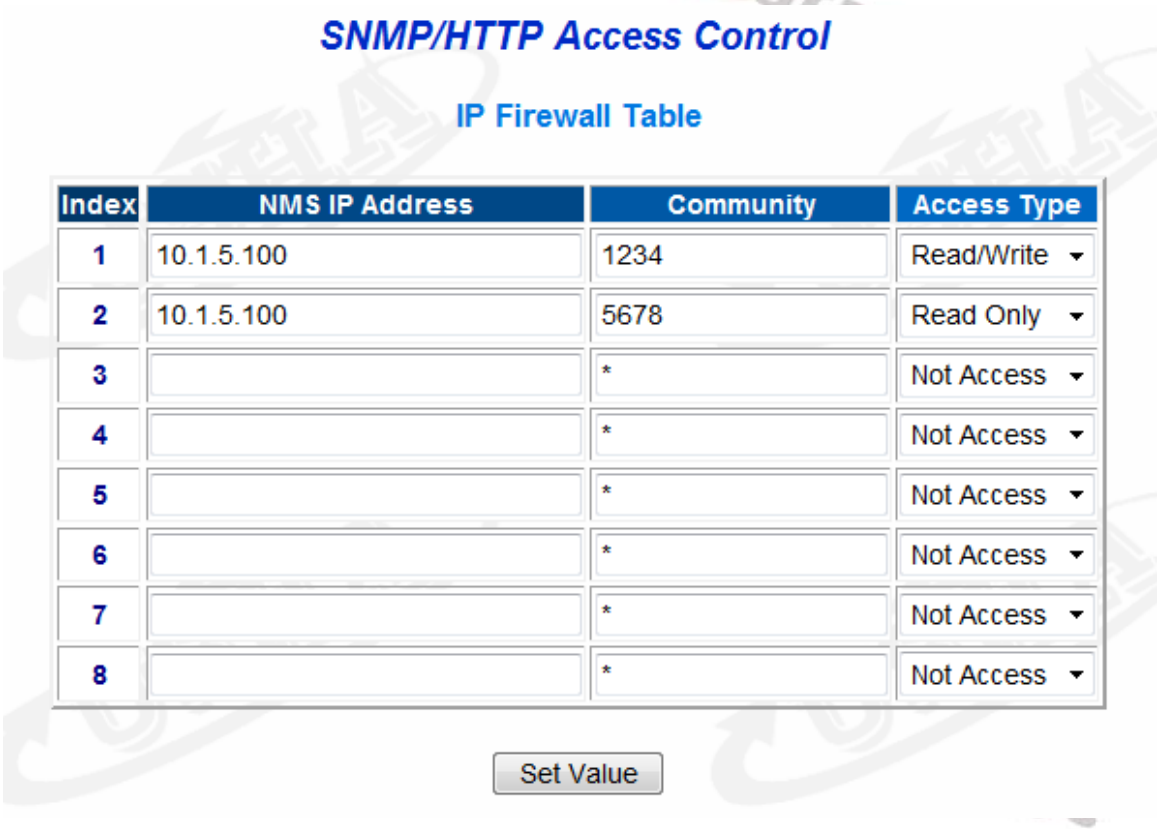

Access IP Address Community String Access
[1] 10.1.7.51 * NotAccess
[2] 10.1.5.87 * Read/Write
[3] * NotAccess
[4] * NotAccess
[5] * NotAccess
[6] * NotAccess
[7] * NotAccess
[8] * NotAccess
COMMANDS -
1. Detail - View the details of a table entry
2. Modify - Modify an entry of table
3. Reset - Reset an entry to default from table
0. Return to previous menu
1
Please Enter Your Choice => 3
Entry Number : 2
2
Access IP Address Community String Access
[1] 10.1.7.51 * NotAccess
[2] * NotAccess
[3] * NotAccess
[4] * NotAccess
[5] * NotAccess
[6] * NotAccess
[7] * NotAccess
[8] * NotAccess
This configuration will be reset
COMMANDS -
1. Detail - View the details of a table entry
2. Modify - Modify an entry of table
3. Reset - Reset an entry to default from table
0. Return to previous menu

2. How to filter

According to different configuration, this function can filter one host or a network segment. You also can set different access type at one host. This function will effect for SNMP and HTTP.

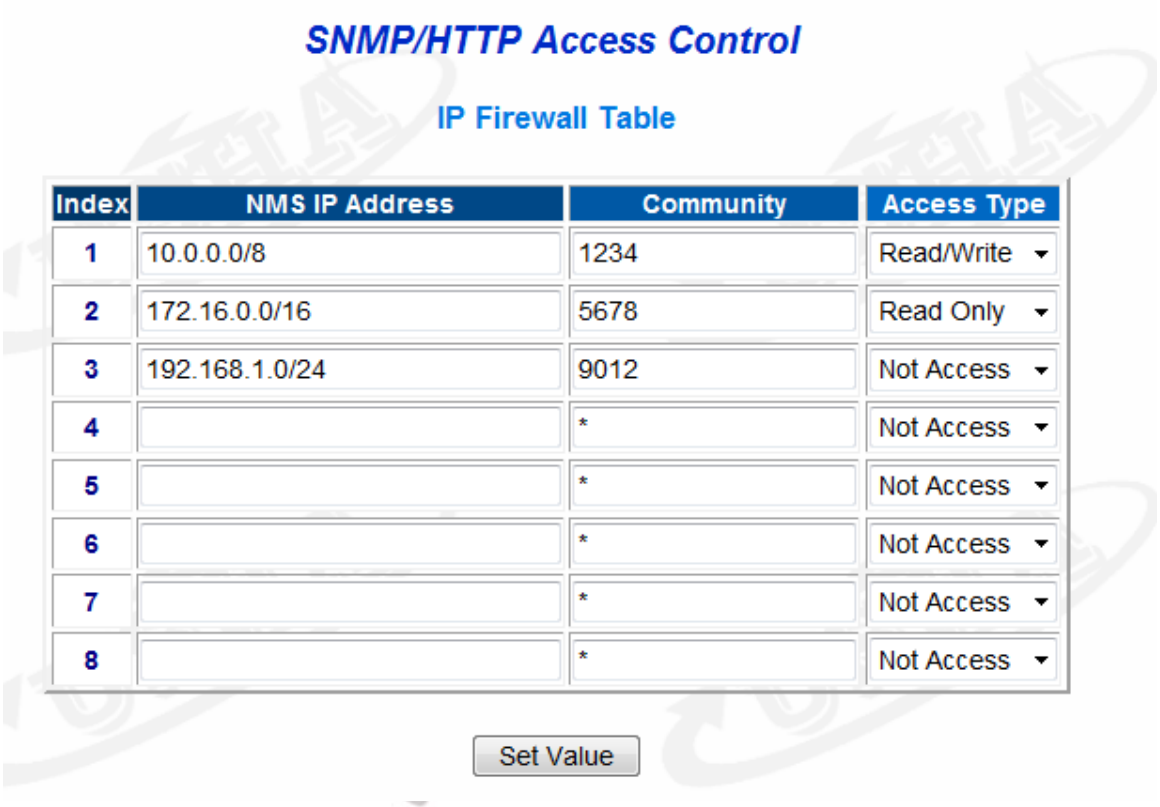
2.1. Host

If you want to management one host, you can set as below table. You can set two passwords correspond to different access type. If you enter community Read/Write password, you can set and read value; if you enter Community Read-Only password, you just read, but not set value. If you login by read-only password and you want to set value, you need login again and enter read/write password.



2.2. Network segment

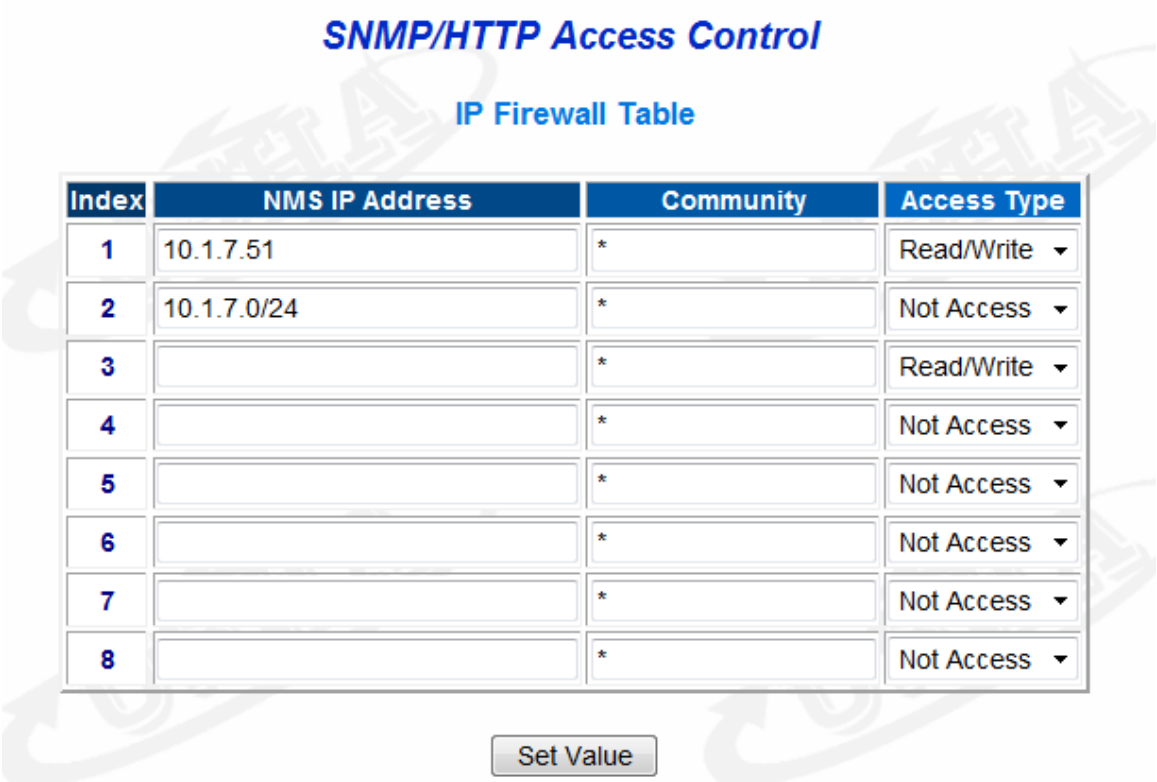
If you want allow or deny a segment, you can set as below. This setting can allow all IP to login and set value in 10.X.X.X segment, and allow all IP to login in 172.16.X.X segment. All IP in 192.168.1.X will be blocked to login.



※ If you want to set a segment, you can use IP / CIDR format to represent an IPv4 or IPv6 segment. For example, "192.168.0.0/16" IPv4 network addresses range from 192.168.0.0 to 192.168.255.255.

2.3. Allow one IP address to login in segment

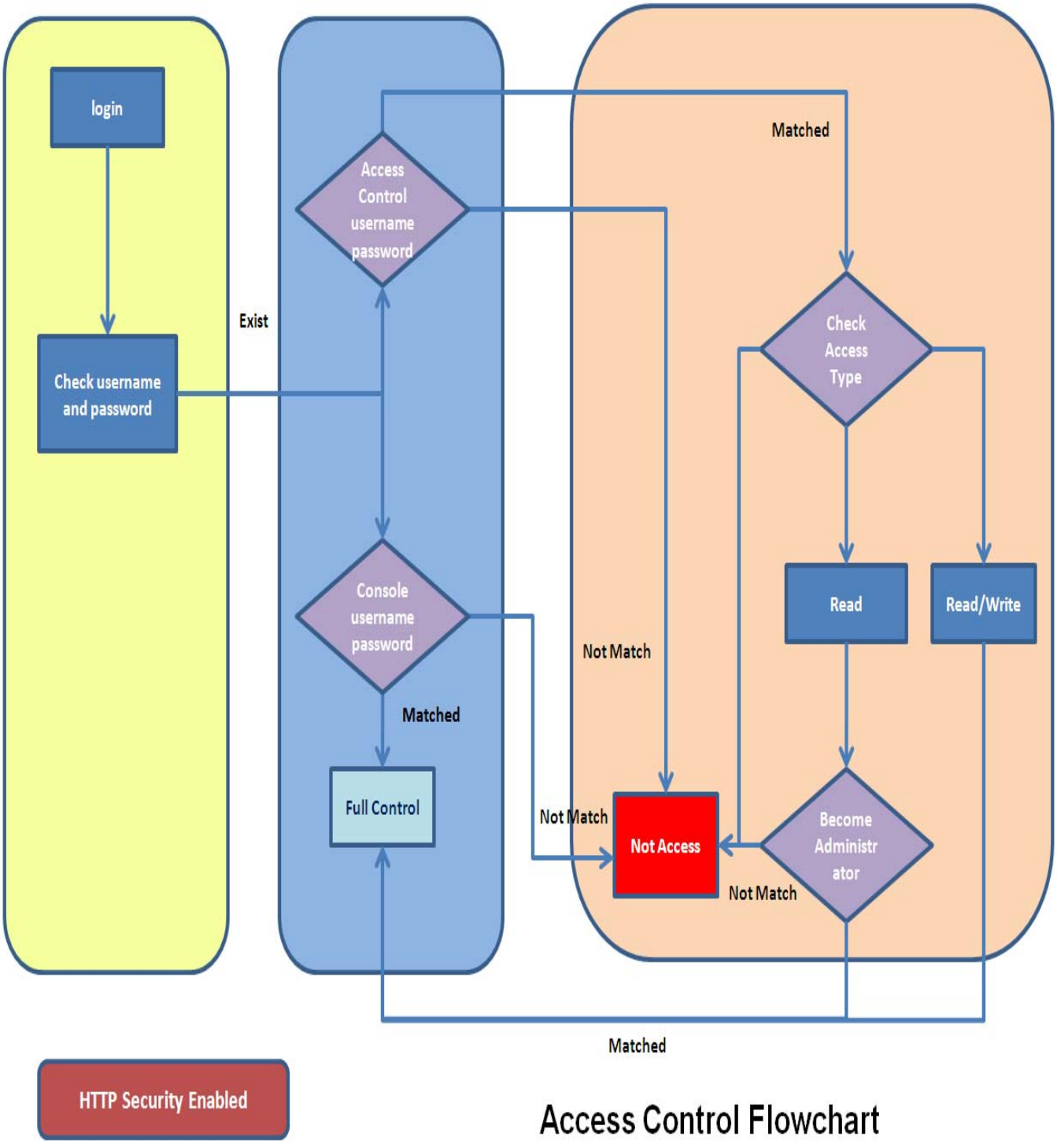
If you just want allow one IP address to login in segment, you can set as below. This setting can block all IP to login in 10.1.7.X segment, except 10.1.7.51.



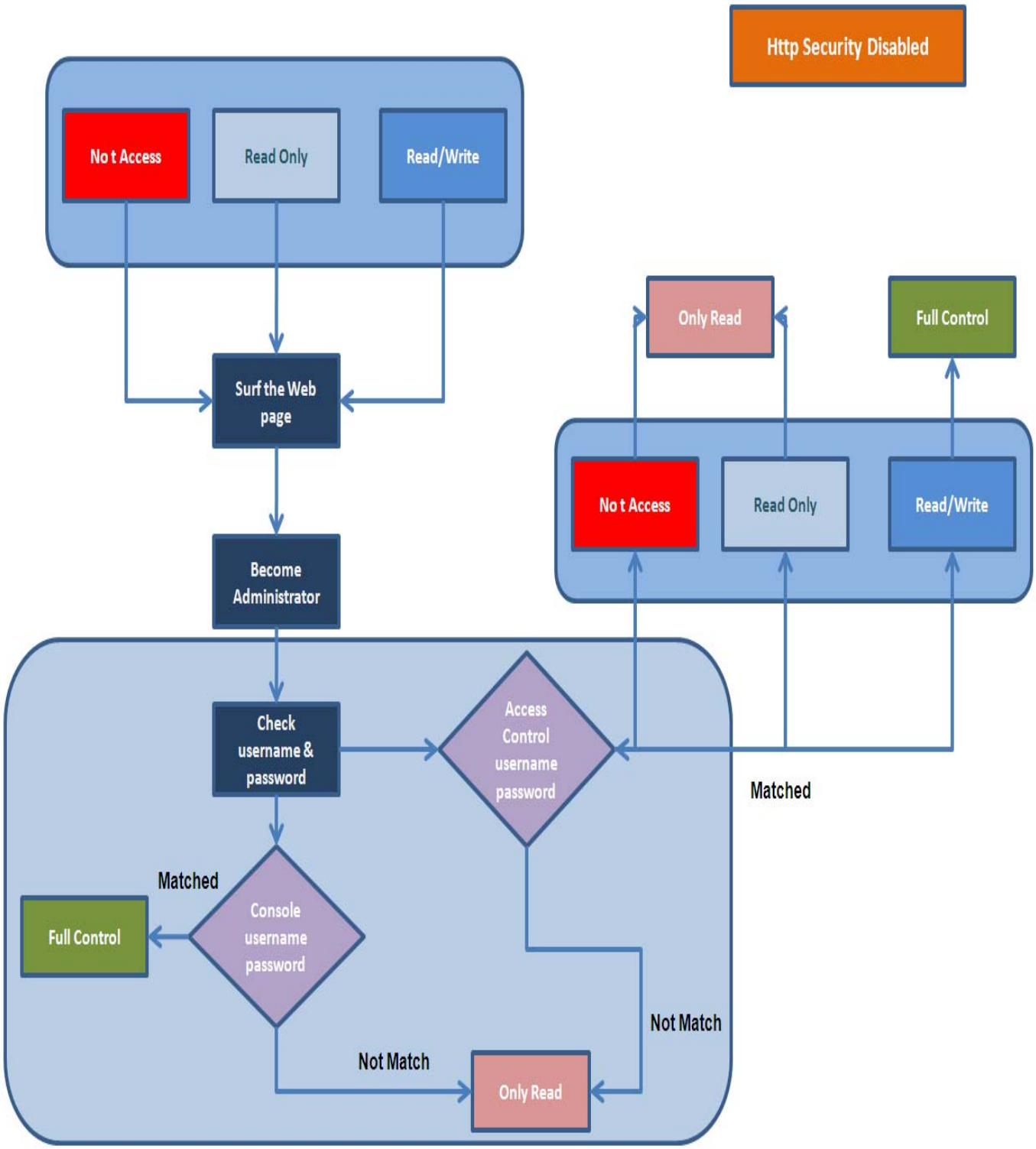
※ Segment must setting at the last one. When host try to connect to USHA, system will compare host IP address and the first condition. If the first condition is match, will not to compare the next condition. So, if segment setting at the first index, it will block 10.1.7.51 login in to USHA.

Appendix A –Behavior flow chart

- **HTTP Security is enabled**



- **HTTP Security is disabled**

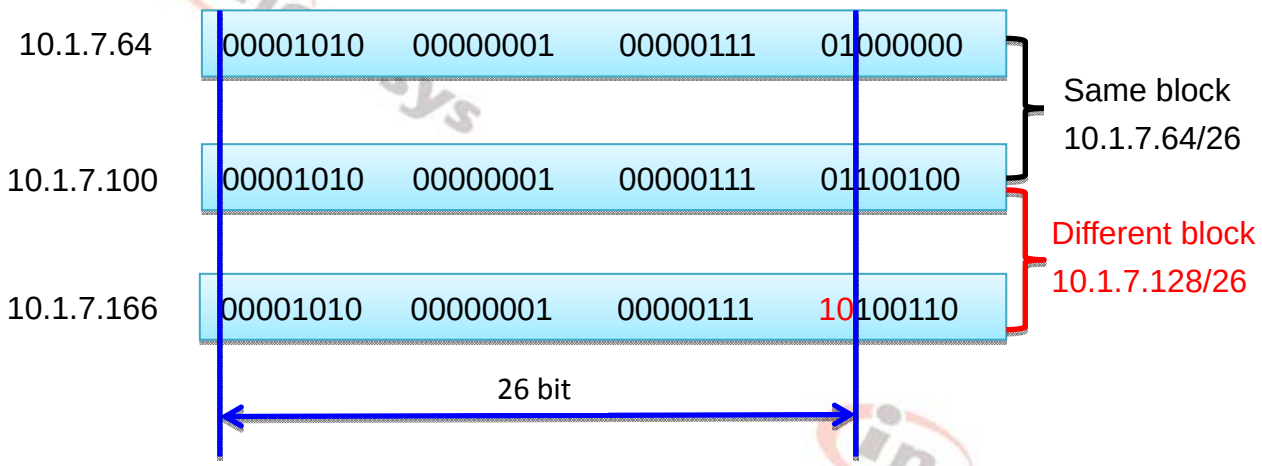


Appendix B – What is IP/CIDR

Classless Inter-Domain Routing (CIDR) is a method for allocating IP addresses and routing Internet Protocol packets. CIDR encompasses several concepts. It is based on the VLSM technique with effective qualities of specifying arbitrary-length prefixes. CIDR notation is syntax of specifying IP addresses and their associated routing prefix. It appends to the address a slash character and the decimal number of leading bits of the routing prefix, e.g., 192.0.2.0/24 for IPv4, and 2001:db8::/32 for IPv6.

- CIDR blocks

An IP address is part of a CIDR block, and is said to match the CIDR prefix if the initial *n* bits of the address and the CIDR prefix are the same. The length of an IPv4 address is 32 bits, an *n*-bit CIDR prefix leaves 32-*n* bits unmatched, meaning that 2^{32-n} IPv4 addresses match a given *n*-bit CIDR prefix. For example, the CIDR address 10.1.7.64/26 indicates a block of 64 IP addresses. So, this segment range is 10.1.7.64 to 10.1.7.127. If we want to know 10.1.7.100 and 10.1.7.166 is the same network segment. We can convert the IP to binary. Because prefix-based 26 bits are different, so 10.1.7.100 and 10.1.7.166 are in different block.



- IPv4 CIDR

IP/CIDR	Mask	IP/CIDR	Mask	IP/CIDR	Mask	IP/CIDR	Mask
a.b.c.d**/32**	255.255.255.255	a.b.c.0**/24**	255.255.255.0	a.b.0.0**/16**	255.255.0.0	a.0.0.0**/8**	255.0.0.0
a.b.c.d**/31**	255.255.255.254	a.b.c.0**/23**	255.255.254.0	a.b.0.0**/15**	255.254.0.0	a.0.0.0**/7**	254.0.0.0
a.b.c.d**/30**	255.255.255.252	a.b.c.0**/22**	255.255.252.0	a.b.0.0**/14**	255.252.0.0	a.0.0.0**/6**	252.0.0.0
a.b.c.d**/29**	255.255.255.248	a.b.c.0**/21**	255.255.248.0	a.b.0.0**/13**	255.248.0.0	a.0.0.0**/5**	248.0.0.0
a.b.c.d**/28**	255.255.255.240	a.b.c.0**/20**	255.255.240.0	a.b.0.0**/12**	255.240.0.0	a.0.0.0**/4**	240.0.0.0
a.b.c.d**/27**	255.255.255.224	a.b.c.0**/19**	255.255.224.0	a.b.0.0**/11**	255.224.0.0	a.0.0.0**/3**	224.0.0.0
a.b.c.d**/26**	255.255.255.192	a.b.c.0**/18**	255.255.192.0	a.b.0.0**/10**	255.192.0.0	a.0.0.0**/2**	192.0.0.0

a.b.c.d**/25**	255.255.255.128	a.b.c.0**/17**	255.255.128.0	a.b.0.0**/9**	255.128.0.0	a.0.0.0**/1**	128.0.0.0